Data Processing Addendum

Version date: December 11, 2025

This Data Processing Addendum (the "**DPA**") is incorporated and forms part of the Order Form and Master Subscription Agreement (or any other agreement governing Customer's use of the InvGate Services) between InvGate and Customer (the "**Agreement**"). Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement.

This DPA outlines the roles, responsibilities, and obligations of the Parties concerning the processing of Personal Data as part of the services provided by the Processor to the Controller.

1. Definitions.

1.1. "**Applicable Data Protection Laws**": refers to any laws and regulations applicable to the processing of Personal Data under the Agreement, including, as applicable, the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act in the United States, Mexico's Federal Law on the Protection of Personal Data Held by Private Parties, Brazil's General Data Protection Law, and Argentina's Personal Data Protection Law.

1.2. "**Controller**": refers to Customer, the entity that determines the purposes and means of processing Personal Data.

1.3. "**Data Breach**": means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.4. "**Data Subject**": means an individual whose Personal Data is being processed.

1.5. "**Personal Data**": means any information relating to an identified or identifiable natural person processed under this DPA, or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Applicable Data Protection Laws.

1.6. "**Processor**": refers to InvGate, the entity that processes Personal Data on behalf of the Controller.

1.7. "**Sub-processor**": refers to any third party engaged by the Processor to assist in processing Personal Data on behalf of the Controller.

2. Scope of Processing.

2.1. **Processing Purposes**. InvGate shall Process Personal Data only to the extent necessary to provide the InvGate Services as set forth in the Agreement. The details of such processing are set out in Schedule 1 herein.

2.2. **Controller Instructions**. The Processor shall process Personal Data only on behalf of the Controller and in accordance with the Controller's documented instructions, as outlined in this DPA and in the Agreement. The Controller represents and warrants that its documented instructions shall comply with Applicable Data Protection Law.

2.3. **Duration of Processing**. The Processor shall process Personal Data for the term of the Agreement, unless otherwise required by law.

3. Processing of Personal Data.

3.1. **Compliance with Laws**. The Processor shall comply with all Applicable Data Protection Laws in processing Personal Data on behalf of the Controller.

3.2. **Confidentiality**. The Processor shall treat Personal Data as Confidential Information under the Agreement. In addition, the Processor shall ensure that all personnel authorized to process Personal Data are subject to appropriate confidentiality obligations.

3.3. **Security Measures**. The Processor has implemented and will maintain appropriate technical and organizational measures to ensure a level of security, confidentiality, integrity and availability appropriate to the risk. InvGate's current security practices are available in the Cloud Security Practices (the "**Security Practices**"). The Security Practices may be updated by InvGate from time to time, provided that such modifications do not materially decrease the overall security of the Solutions. The Controller shall be responsible for configuring the Solutions and managing its own data in order to maintain appropriate security of Personal Data and complying with Applicable Data Protection Laws.

4. Sub-processors.

4.1. **General Authorization**. The Controller hereby grants the Processor a general authorization for the Processor to engage Sub-processors. The Processor shall notify the Controller before authorizing any new Sub-processor. The Controller may object in writing within thirty (30) days of such notice. If the Controller objects, the Processor shall use commercially reasonable efforts to provide an alternative or propose change to the InvGate Services to avoid processing by the objected-to Sub-processor. If no alternative is available within sixty (60) days, the Controller may terminate the affected Order Form(s) with respect to the impacted InvGate Services by written notice.

4.2. **Sub-processor Contracts**. The Processor shall ensure that all Sub-processors are bound by written agreements that impose obligations equivalent to those set forth in this DPA.

4.3. **Liability**. The Processor shall remain liable vis-à-vis the Controller for any breaches of the Sub-processors' data protection obligations with regard to the processing activities herein.

5. Data Subject Rights.

5.1. **Assistance with Requests**. The Processor shall reasonably assist the Controller in responding to requests from Data Subjects to exercise their rights under Applicable Data Protection Laws, including rights to access, rectification, deletion, data portability, and restriction of processing, as long as they are related to the processing of Personal Data made by the Processor.

5.2. **Notification of Requests**. Unless prohibited by law, if the Processor receives a request from a Data Subject, the Processor shall forward such request to the Controller.

6. Security Incidents.

6.1. **Notification**. In the event of a Data Breach, the Processor shall notify the Controller without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the Data Breach.

6.2. **Mitigation**. The Processor shall take all reasonable measures to mitigate the effects of the Data Breach and assist the Controller by providing information reasonably necessary for the Controller to meet its obligations under Applicable Data Protection Laws.

7. Data Retention and Deletion.

7.1. **Data Deletion**. Upon expiration of the Agreement, the Processor shall delete or return to the Controller all copies of Personal Data, except where continued retention is required by law.

7.2. **Backups**. The Processor may retain backup copies of Personal Data for a limited period following the expiration of the Agreement, subject to continued confidentiality and data protection obligations as set forth herein and in the Agreement.

8. Audit Rights.

8.1. **Audits**. The Processor is regularly audited by independent third-party auditors. Upon the Controller's request, the Processor shall make available to the Controller appropriate information to evidence the Processors' compliance with this DPA. In the event that the Controller is not able to reasonably verify the Processor's compliance with this DPA with the evidence provided by the Processor, the Processor shall provide written responses (on a confidential basis) to the Controller for any reasonable and specific questions that are not covered by the documentation previously provided.

8.2. **On-site Audits**. In the event that after following the process set forth in Section 8.1 the Controller is still unable to reasonably verify the Processor's compliance with this DPA, then the Controller may, at Controller's expense, conduct an on-site audit provided that: (i) is conducted during regular business hours at the Processor's time zone (UTC-3) in a manner designed to minimize disruption to the Processor's operations; (ii) is required by the Controller in writing at least sixty (60) days in advance; (iii) is subject to confidentiality controls that obligates the Controller to keep confidential any information or result of such audit; and (iv) occurs no more than once a year.

9. Term and Termination.

9.1. **Termination of the DPA**. This DPA shall automatically terminate upon the expiration of the Agreement. Notwithstanding the foregoing, the obligations of the Processor regarding data protection and confidentiality shall continue for as long as the Processor retains Personal Data.

10. Liability.

10.1. **Limitation of Liability**. The limitation of liability provisions set forth in the Agreement shall apply *mutatis mutandi* to this DPA. Without limiting the generality of the foregoing, the Processor shall not be liable for any data processing activities that were conducted in accordance with the Controller's instructions.

11. International data transfer.

11.1. **Standard Contractual Clauses**. Where applicable, any transfer of Personal Data from the European Economic Area ("**EEA**"), the United Kingdom, or Switzerland to a country outside the EEA that is not subject to an adequacy decision shall be governed by the standard contractual clauses for the transfer of Personal Data to third countries provided for in article 46 of GDPR, which are hereby incorporated into this DPA by reference.

12. Miscellaneous.

12.1. **Conflicts**. In the event of any conflict between the terms of this DPA and the Agreement, the terms of this DPA shall prevail with regards to the provisions relating to the processing of Personal Data.

12.2. **Modifications**. The Processor may modify this DPA from time to time by updating the appropriate sections in the Processor's website. The Controller shall have the right to reject the modifications to this DPA by giving written notice to InvGate within thirty (30) days of such modifications taking effect. In the event the Controller rejects the modifications, the Parties shall continue to be governed by the terms of the prior version of the DPA. The Controller's continued use of the InvGate Services following the effective date of any modification without a written notice rejecting them shall be understood as the Controller's consent to such modifications.

12.3. **Governing Law**. This DPA shall be governed by the laws governing the Agreement.

Schedule 1

Detail of Processing Activities

1. **Nature of Processing**. Provision of InvGate's cloud-based IT Service Management and IT Asset Management solutions, together with associated services, including implementation, configuration, technical support, maintenance, and service-related analytics necessary to deliver and improve the contracted services.

2. **Purpose of Processing**. Hosting, storage, backup, technical support, and related activities necessary to provide the contracted services and service-related improvements.

3. **Types of Personal Data**. Personal Data processed may include:

   - Identification and contact details of Controller's authorized users (such as name, email address, and job title).
   - Any Personal Data voluntarily included by the Controller or its users in support tickets or related communications.
   - Any other Personal Data that the Controller or its users choose to upload or submit to the Solutions as Service Data, to the extent necessary for providing the services.

   For the avoidance of doubt, the nature and scope of Service Data uploaded to the Solutions are determined solely by the Controller and its users, and the Processor does not control the type of Personal Data processed.

4. **Categories of Data Subjects**. Personal Data processed may relate to the following categories of Data Subjects:

   - The Controller's authorized users (e.g., employees, contractors, or agents who are granted access to the Solutions).
   - Other individuals whose Personal Data the Controller or its users choose to upload to the Solutions in connection with their use of the services.

5. **Duration of Processing.** Personal Data will be processed for the duration of the Subscription Term and will be deleted or returned in accordance with the provisions of the Agreement.